

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

Hon. Hugh B. Scott

v.

14CR42A

Order

JOSEPH S. HELENIAK,

Defendant.

This matter has been referred to the undersigned pursuant to 28 U.S.C. § 636(b)(1)(C) (text Referral Order, dated Mar. 5, 2014). The instant matter before the Court is defendant's omnibus motion (Docket No. 37), including his motion to suppress statements of defendant's admission to possession of child pornography; suppress evidence from search warrant; and to controvert the search warrant. This Court here considers whether a hearing is in order for these forms of relief. Other relief (service of a Bill of Particulars, identification of informants, production of discovery, production of Jencks Act material and Brady material, production of Federal Rules of Evidence 404(b), 608, 609, preservation of rough notes, and production of Grand Jury transcripts) will be addressed in a separate Order upon determination that all briefing on the motion is deemed submitted.

BACKGROUND

Defendant was charged with transportation of child pornography in interstate commerce, in violation of 18 U.S.C. § 2252A(a)(1) and (b)(1), on various dates in 2013 and 2014, and

possession of child pornography on those dates, in violation of 18 U.S.C. § 2252(a)(5)(B) and (b)(2). (Docket No. 18, Indict.). The Indictment also charged a criminal forfeiture of visual depictions of child pornography (id.).

The alleged pornography at issue was distributed through email by an AOL account. As the Government explains (Docket No. 39, Gov't Response at 1-4), AOL as service provider requires subscribers to agree to terms of service that users comply with applicable laws and not use AOL's facilities to conduct illegal activity, in particular to not post content that is explicit or graphic descriptions of sexual acts. AOL states that, to avoid violations and to enforce the terms of service, it will take any technical, legal, or other actions deemed necessary without notice to the user (id. at 1-2, Ex. 1, AOL terms of service). In United States v. DiTomasso, No. 14-cr-160 (SAS), 2014 U.S. Dist. LEXIS 152505, at *4-5, 27 (S.D.N.Y. Oct. 28, 2014), Judge Scheindlin found that AOL, in its Member Community Guidelines, id. at *4 n.13, had reserved the right to take any action deemed warranted to prevent illegal activity, including cooperating with law enforcement (see Docket No. 51, Gov't Response at 2, Ex. 1, AOL Member Community Guidelines).

Among techniques used by AOL is a scanning tool called Image Detection and Filtering Process ("IDFP") to compare the hash value (or a unique numeric identifier for digital computer files) of scanned email with known files containing apparent child pornography (id. at 2). When IDFP makes a match of hash values for a known pornographic file, the suspected email is reported to the National Center for Missing and Exploited Children (or "NCMEC") CyberTipline, pursuant to 18 U.S.C. § 2258A(a)(1) (id. at 2 & n.1; see Docket No. 37, Def. Atty.

Affirm. ¶ 101). NCMEC was founded in 1984 under the Missing Children's Assistance Act (Docket No. 37, Def. Atty. Affirm. ¶ 175).

Federal Bureau of Investigation task force officer Michael Hockwater swore an affidavit in support of a federal search warrant that, AOL, in detecting a suspicious file and reporting it to NCMEC, does not inspect the contents of the electronic file to determine whether child pornography exists (Docket No. 37, Def. Atty. Affirm. ¶ 101). The Government later concedes that it learned from AOL that AOL, in fact, did physically review the suspected files before sending them to NCMEC (Docket No. 39, Gov't Response at 4 n.4). NCMEC then inspects the file to confirm the presence or absence of child pornography and then reports this information to law enforcement (Docket No. 37, Def. Atty. Affirm. ¶ 101; Docket No. 39, Gov't Response, Ex. 4).

In this case, on September 3, 2013, AOL submitted a report to NCMEC declaring that an AOL user submitted an e-mail with three attachments containing suspicious images of child pornography sent to the same e-mail address (Docket No. 37, Def. Atty. Affirm. ¶ 102; Docket No. 39, Gov't Response at 4). NCMEC representatives then reviewed the e-mail and attachment and concluded that it contained child pornography (Docket No. 37, Def. Atty. Affirm. ¶ 102), referring the matter to the New York State Attorney General's office. On November 4, 2013, New York State Police investigator John Lombardi viewed the images from the NCMEC CyberTipline Report, confirming that these images were child pornography (Docket No. 39, Gov't Response at 5-6). On January 3, 2014, Lombardi confirmed the AOL user was the defendant living in West Seneca, New York, and the Federal Bureau of Investigation was contacted for a possible federal prosecution (*id.* at 6).

On January 23, 2014, this Court issued a search warrant for the premises of 174 Broadway Road, West Seneca, New York, defendant's residence (Docket No. 37, Def. Atty. Affirm. ¶ 100). That warrant was executed on January 24, 2014. Defendant was not in custody when the warrant was executed and defendant volunteered to be interviewed. During the interview, defendant allegedly admitted to searching for and downloading child pornography for the past eight months; he would find images, copy and e-mail them to himself. (Docket No. 39, Gov't Response at 6.) Defendant was shown the three images from the CyberTipline Report and he confirmed that he e-mailed those images to himself (id.). Defendant provided a written statement (id., Ex. 5) wherein he identified his AOL e-mail address (the same as the one reported in the NCMEC report), admitted that he looked at and e-mailed child pornography. During the execution of the warrant, defendant's computer was seized and a subsequent forensic examination found ten images of alleged pornography (Docket No. 39, Gov't Response at 6). This forensic examination also revealed that, after AOL terminated defendant's account, he upgraded his operating system to Windows 8, which would have deleted all child pornography actively saved on the computer (id. at 6-7). Following execution of the search warrant, defendant was arrested and charged in a criminal complaint (Docket No. 1) with receipt of child pornography (Docket No. 39, Gov't Response at 7). On January 29, 2014, a second search warrant was executed for defendant's former AOL account, revealing that three times e-mails were sent from that AOL address back to that address with child pornography attachments (id.), including the three images in the NCMEC report. In another e-mail, defendant sent himself an e-mail with ten attachments of child pornography (id.).

Defendant's Suppression Motion

Within defendant's omnibus motion (Docket No. 37), defendant seeks to controvert the search warrants for the search of the house and for the AOL account (id., Def. Atty. Affirm. ¶¶ 102-07, 108-09, 110). Defendant sought an Order that the Government describe the process (discussed above) for AOL's involvement in this matter (id. ¶ 111). Defendant argues that NCMEC is a Government agency and thus AOL is an agent of the Government and that NCMEC's review was done without a prior search warrant (id. ¶¶ 113, 175; see Docket No. 50, Def. Atty. Aff. ¶ 5). Defendant seeks a hearing regarding the argued warrantless search and seizure of the images cited in the supporting affidavit for the search warrant (Docket No. 37, Def. Atty. Affirm. ¶ 150). Defendant wants this Court to find whether the acts of AOL "were based upon a relationship it had with federal authorities," whether NCMEC's review of the e-mail without a warrant violates defendant's Fourth Amendment rights; whether the subsequent search warrants should be controverted and evidence suppressed and whether the warrants were tainted by these unlawful acts (id. ¶ 170).

Defendant also contends that Attachment B to the search warrant renders the subsequent search general (id. ¶ 115) because the supporting affidavit was not incorporated by reference to the warrant to restrict its scope (id. ¶ 118). Even if the affidavit is referred to, defendant contends that it provides no guidance and this Court's authorization became general and an exploratory search of defendant's home (id. ¶ 132). Defendant also denies that probable cause exists to justify the search (id. ¶ 133). Defendant seeks a hearing as to the appropriateness of the seizure of all images on defendant's computer, since defendant argues this exceeds the scope

permitted by the warrant (id. ¶ 135), see United States v. Galpin, 720 F.3d 436 (2d Cir. 2013) (searches of computer hard drive requires particularity) (id. ¶¶ 136-47).

Defendant also challenges the conclusory allegations of agent Hochwater of the ages of the youths depicted in the images at issue, claiming that they appeared to be under 16 (id. ¶¶ 153-57) without any basis (factual or expert) for that finding (id. ¶ 162).

In response, the Government first denied that defendant was in custody when he made his oral and written statements to Government agents conducting the search of his house (Docket No. 39, Gov't Response at 8-9). The Government insists upon an affidavit from a person with factual knowledge to support defendant's motion for an evidentiary hearing (id. at 10). Defense counsel later stated that defendant will file an affidavit regarding the execution of the search warrant (Docket No. 50, Def. Atty. Aff. ¶¶ 3, 9).

In reply, defendant points out that the Government concedes that in one case, United States v. Keith, 980 F. Supp. 2d 33, 40 (D. Mass. 2013), that NCMEC was found to be a Government agent when it provides information to law enforcement (Docket No. 50, Def. Atty. Aff. ¶ 10).

DISCUSSION

I. Suppression of Statement

A. Private Party as Government Agent

The Fourth Amendment's guarantee to be free from unreasonable search and seizure is directed at Government activity, see, e.g., United States v. Jacobsen, 466 U.S. 109, 113 (1984); United States v. Richardson, 607 F.3d 357, 364 (4th Cir. 2010). "However, when a private individual conducts a search 'as an instrument or agent of the Government,' Skinner v. Railway

Labor Executives' Ass'n, 489 U.S. 602, 614 (1989), the limits imposed by the Fourth Amendment apply,” Richardson, supra, 607 F.3d at 364 (also citing United States v. Jarrett, 338 F.3d 339, 344 (4th Cir. 2003)). Whether a private individual serves “as a mere conduit for the Government to perform a search ‘necessarily turns on the degree of the Government’s participation in the private party’s activities,’” Richardson, supra, 607 F.3d at 364 (quoting Skinner, supra, 489 U.S. at 614), where some evidence of Government participation or affirmative encouragement of the private search is required before that search is held to be unconstitutional, id. (quoting Jarrett, supra, 338 F.3d at 346). A private person “cannot act unilaterally as an agent or instrument of the state; there must be some degree of governmental knowledge and acquiescence,” United States v. Shewin, 539 F.2d 1, 6 (9th Cir. 1976) (en banc), cert. denied, 437 U.S. 909 (1978); United States v. Bennett, 709 F.2d 803, 805 (2d Cir. 1983) (quoting Shewin).

Defendant argues here that private entities AOL and NCMEC acted as Government agents in and conducted a warrantless search leading to obtaining the search warrant (Docket No. 37, Def. Atty. Affirm. ¶ 113), thus the warrants are void because they were based on this warrantless information (id.). Defendant argues that NCMEC is a Government agent, citing (as does the Government, Docket No. 39, Gov’t Response at 20-21), United States v. Keith, 980 F. Supp. 2d 33, 40, 41-42 (D. Mass. 2013) (Docket No. 50, Def. Atty. Aff. ¶ 10).

In Keith, the United States District Court for the District of Massachusetts found that AOL did not open the suspected e-mail (instead it compared hash value of the file with a database of stored hash value of offending files, id. at 40) and thus was not a Government agent, while NCMEC, which opens and examines suspected material, was a Government agent. The

Keith court noted that NCMEC, while not officially a Government entity, receives a grant from the Government which is used (among other purposes) to operate the CyberTipline and forward reports of child pornography to the Government, noting a “not just rhetorical but real” partnership between NCMEC and the Government, id. at 41 (quoting United States v. Cameron, 699 F.3d 621, 644 (1st Cir. 2012)). The Keith court expressly distinguished matching the hash value of a file from opening it and viewing its contents, since the hash value match does not confirm the provenance of the contents of a file to contain, id. at 43. In Stevenson, the court held that the reporting obligation AOL has to NCMEC by itself does not transform AOL into a Government agent, 727 F.3d at 830; accord Cameron, supra, 699 F.3d at 637-38; Richardson, supra, 607 F.3d at 366-67.

The District of Montana distinguished Google from AOL in United States v. Drivdahl, No. CR-13-18-DLC, 2014 U.S. Dist. LEXIS 29233 at *12 (D. Mont. Mar. 6, 2014), because Google opened the suspect material while AOL in Keith relied solely upon the algorithmic hash value information to identify suspect items and did not open the actual e-mails. The Drivdahl court went on to find that Google was not a Government agent because the Government was not aware of Google’s investigation “let alone acquiesced or encouraged it—until it was completed and sent” to NCMEC, 2014 U.S. Dist. LEXIS 29233, at *8 (applying standard whether private party’s search implicated the Fourth Amendment, see United States v. Cleaveland, 38 F.3d 1092, 1093 (9th Cir. 1994)).

The Government cites various cases that held that AOL (or like internet service providers) was not a Government agent when they implement their own internal security measures against users engaging in illegal activity through their services (Docket No. 39, Gov’t

Response at 20-21), see United States v. Richardson, 607 F.3d 357, 364 (4th Cir. 2010); United States v. Stevenson, 727 F.3d 826, 829-30 (8th Cir. 2013); Keith, supra, 980 F. Supp. 2d at 40 (AOL is not an agent); United States v. Ackerman, No. 13-10176-01-EFM, 2014 U.S. Dist. LEXIS 89243 (D. Kan. July 1, 2014); Drivdahl, supra, No. CR-13-18-DLC, 2014 U.S. Dist. LEXIS 29233 (D. Mont. Mar. 6, 2014) (Google is not a Government agent); see also Cameron, supra, 699 F.3d at 637-38 (Yahoo!, Inc., did not act as an agent in searching e-mails and sending reports to NCMEC); United States v. DiTomaso, No. 14-cr-160(SAS), 2015 U.S. Dist. LEXIS 9645, at *2 (S.D.N.Y. Jan. 26, 2015) (chat service provider Omegle held not to be a Government agent and its search of defendant's chat messages held to be a pure private search beyond the reach of the Fourth Amendment); cf. Keith, supra, 980 F. Supp. 2d at 41-42 (NCMEC is an agent). The Government also argues that, pursuant to the terms of AOL's terms of service, plaintiff consented to the search of his e-mails despite having an expectation of privacy in those missives (Docket No. 51, Gov't Response at 2), DiTomaso, supra, 2014 U.S. Dist. LEXIS 152505, at *27-28.

The Government then admits in a footnote in this case that AOL in fact opened the e-mail that it forwarded to NCMEC (Docket No. 39, Gov't Response at 4 n.4). Thus, AOL in this case is in the same circumstances as NCMEC in that both agencies actually opened the e-mail to see if offense materials were contained. But the Government argues that defendant consented to the search by AOL by agreeing to AOL's terms of service and community guidelines (Docket No. 51, Gov't Response at 2, Ex. 1 (AOL Community Guidelines); see Docket No. 39, Gov't Response, Ex. 1 (AOL's Terms of Service)).

The Government argues that AOL's status must be considered first and NCMEC's status need not be reached. But two different searches were conducted by each entity. AOL, either by comparing hash values or by actually reviewing e-mail scrutinized defendant's messages and then conveyed the suspicious e-mail to NCMEC. NCMEC then conducted its own investigation, opening the e-mail and reviewing the attachments. The fact that this is a chain of private searches does not prevent this Court from considering the constitutionality of the searches involved. As discussed below regarding the argument that defendant consented to AOL's search, that argument only addresses one of two actions. Similarly, the AOL search does not insulate the subsequent NCMEC search from scrutiny.

Defendant seeks a full evidentiary hearing to determine whether Government agents had contact with NCMEC leading up to the issuance of the search warrants in this case (Docket No. 50, Def. Atty. Aff. ¶ 13). This Court notes that at least one of the courts cited by the parties held a hearing on this issue, see Ackerman, supra, 2014 U.S. Dist. LEXIS 89243, at *1, 2 n.1 (NCMEC appeared through counsel and filed an amicus brief). Defendant also controverts the warrant, but this is directly connected to how the warrant was obtained based upon AOL and NCMEC's actions. A hearing is thus warranted. Fact issues exist as to whether the Government was aware of, acquiesced in, or encouraged either AOL or NCMEC's internal security measures in reviewing defendant's e-mail; whether either AOL or NCMEC were Government agents in conducting this search.

B. Defendant's Consent as User of AOL

A further issue is whether defendant's agreement to AOL's terms of service and community guideless constitutes consent to a search. Cooperation with law enforcement is not

defined in either document. Consent need not be a knowing waiver of Fourth Amendment rights, but it must be voluntary and that voluntariness is determined upon a review of the totality of the circumstances, Schneckloth v. Bustamonte, 412 U.S. 218, 226, 241-42 (1973); United States v. Wilson, 11 F.3d 346, 351 (2d Cir. 1993). The Government bears the burden of demonstrating that consent was voluntarily given, United States v. Isiofia, 370 F.3d 226, 230 (2d Cir. 2004), and “because defendants frequently claim that their consent was obtained involuntarily or not at all, a judge’s decision on the issue will often boil down to a credibility” determination, Gordon Mehler, John Gleeson, and David C. James, Federal Criminal Practice: A Second Circuit Handbook 661 (14th ed. 2014). A number of factors are relevant to determine voluntariness, including the setting in which consent is obtained, Schneckloth, supra, 412 U.S. at 226; Mehler, Gleeson & James, supra, at 661. Furthermore, the scope of any consent to search “is measured by what a reasonable person would have understood based upon the discussion between the officer and the person giving consent,” Mehler, Gleeson & James, supra, at 662; see Florida v. Jimeno, 500 U.S. 248, 250-51 (1991).

Here, the setting differs from most criminal cases because the consent is given not directly to a Government investigator but to a third party, as a condition of use of the service provided by that third party. As Judge Scheindlin posed in DiTomasso, supra, 2014 U.S. Dist. LEXIS 152505, at *24 (emphasis in original omitted), the question is “what [the typically reasonable person] consented to” by agreeing to AOL’s terms of service, whether he consented to a search by AOL in a law enforcement capacity, id. at *24-25. The text of both the terms of service and the community guidelines are very general and do not state that others may be involved in the screening of a member’s e-mail to enforce legal and AOL member standards.

The Government relies upon DiTomasso (Docket No. 51, Gov't Response at 2) and its holding that, while there is constitutionally recognized expectation of privacy in e-mails, 2014 U.S. Dist. LEXIS 152505, at *11-18, 24, the defendant there consented to AOL's search as a Government agent when that defendant accepted AOL's terms of use notifying him of AOL's cooperation with the Government, id. at *24-28, concluding that "a reasonable person familiar with AOL's policy would understand that by agreeing to the policy, he was consenting not just to monitoring by AOL as an ISP, but also to monitoring by AOL as a government agent," id. at *28. Even if this Court accepts that conclusion, there are issues of fact whether this defendant was familiar with AOL's policy to make his use of the service consent to search by a Government agent. Even if, by using AOL's services defendant consented to AOL's search and cooperation with the Government, that consent may not include consenting to a search by a third party (NCMEC) and reference of his e-mails to another government (here, referral to the New York State Attorney General). This Court disagrees with the Government that this issue can be decided as a matter of law. Whether this defendant consented to AOL searching his e-mail as a Government agent raises questions of fact for an evidentiary hearing.

II. Defendant's Statement

As to an evidentiary hearing for suppression of defendant's statements during the execution of the search warrant, the Government contends that defendant has not presented an affidavit from a person with knowledge of the interview to warrant a hearing (Docket No. 39, Gov't Response at 10), and here there is no affidavit from defendant himself. Defense counsel offered to submit his client's affidavit (Docket No. 50, Def. Atty. Aff. ¶ 3) following argument where defendant acknowledged and adopted defense counsel's contentions.

CONCLUSION

Based upon the above, defendant's motion for an evidentiary hearing as to his motions for suppression of evidence (Docket No. 37, Def. Atty. Affirm. ¶¶ 136-47; see Docket No. 50, Def. Atty. Aff. ¶¶ 13-17) is **granted**; the date of the hearing will be set in a separate Order.

SO ORDERED.


Hon. Hugh B. Scott
United States Magistrate Judge

Dated: Buffalo, New York
February 9, 2015